UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/714,101	11/14/2003	Craig Partridge	02-4122	9540

7590 03/18/2009

Verizon Corporate Services Group Inc.
600 Hidden Ridge
HQE03H01
Irving, TX 75038

EXAMINER	
ZIA, SYED	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
03/18/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/714,101	PARTRIDGE ET AL.	
	Examiner	Art Unit	
	SYED ZIA	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 December 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-82 and 84* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-82, and 84* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This office action is in response to remarks file on December 9, 2008. Original application contained Claims 1-84. Applicant cancelled Claim 83. Therefore, Claims 1-82, and 84 are pending for consideration.

Claim Rejections - 35 USC § 101

Rejection under 35 U.S.C. 101 has been withdrawn.

Response to Arguments

Applicant's arguments filed December 9, 2008 have been fully considered but they are not persuasive because of the following reasons: Applicant stated that the effective filing date of the present application is December 27, 2002 while the filing date of cited prior art is July 11, 2003. This is not found persuasive, cited prior art was filed on July 11, 2003 and also claims benefit to provisional patent application serial number 60/395,838, filed on July 12, 2002. Therefore, the effective filing date of the cited prior art application is July 12, 2002 which is prior to the filing date of present application (December 27, 2002).

Accordingly, rejection for Claims 1-82 and 84 is respectfully maintained

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-82, and 84 are rejected under 35 U.S.C. 102(e) as being anticipated by Hamadeh et al. (U. S. Publication No.: 2004/0093521 A1).

1. Regarding Claim 1 Hamadeh teaches and describes a method for facilitating reduction of a security threat in connection with transmission of an IP datagram having an IP header and an identification field in the IP header comprising: supplementing the identification field of the IP header with at least one bit from another field of the EP header, whereby probability of random collisions is reduced, thereby reducing the security threat in connection with the transmission of the IP datagram [0125 - 0148].

2. Regarding Claim 2 Hamadeh teaches and describes method for formatting an IP datagram having an IP header containing an identification field comprising: a. determining identification information having a length greater than 16 bits associated with data to be sent in the IP datagram; b. inserting at least one bit of the identification information into the identification field of the header; and C. inserting remaining bits of the identification information into at least one

other field of the header [[0125 - 0148].

3. Regarding Claim 11 Hamadeh teaches and describes method for formatting an IP datagram having an IP header comprising: a. determining a special value based on a secret shared with a destination node; and b. inserting at least a part of the special value into identification information carried by the header for the IP datagram, wherein a first portion of the identification information is included in the an identification field of the header and a second portion of the identification information is included in at least one other field of the header [0125 - 0148].

4. Regarding Claim 18 Hamadeh teaches and describes a method for facilitating fragmentation-free transmissions between two IPsec nodes implementing IPsec protocol, the method comprising: a. transmitting a plurality of packets of differing size from a first IPsec node to a second IPsec node, each packet having an IP header wherein a "Don't Fragment" (DF) bit in a fragmentation flag field in the header for each packet of the plurality is set to a value that is arranged to prevent fragmentation of the packet en route; and b. determining a maximum packet size for avoiding fragmentation in transmissions from the first IPsec node to the second IPsec node based on at least one response from the second IPsec node to the plurality of packets transmitted by the first IPsec node [0125 - 0148].

5. Regarding Claim 20 Hamadeh teaches and describes a method for assembling a plurality of received IP datagrams each having an IP header comprising: assembling the plurality of

received IP datagrams based on identification information contained in an identification field and at least one other field of the header for each of the received IP datagrams, wherein the identification information for each received IP datagram does not include source address information, destination address information or protocol information for that received IP datagram [0125 - 0148].

6. Regarding Claim 22 Hamadeh teaches and describes a method for assembling IP datagrams each having an IP header, the method comprising: a. receiving a plurality of the IP datagrams; b. extracting identification information from each of the plurality of the IP datagrams, the identification information for each of the IP datagrams comprising 16 bits of an identification field and at least one bit from at least one other field of the header for that IP datagram, the at least one bit not including source address information, destination address information or protocol information for the IP datagram; c. identifying a subset of the plurality of the IP datagrams based on the identification information and at least one element selected from the group consisting of the source address information, the destination address information and the protocol information for each IP datagram from the subset; and d. assembling the subset of the plurality of the IP datagrams into a message based on fragmentation offset information from a fragmentation offset field of the header for each IP datagram from the subset [0125 - 0148].

7. Regarding Claim 26 Hamadeh teaches and describes a method for facilitating fragmentation-free transmissions between two IPsec nodes implementing IPsec protocol, the method comprising: a. receiving a plurality of packets of differing size from a first one of the

IPsec nodes at a second one of the IPsec nodes, each of the packets having an IP header; wherein a "Don't Fragment" (DF) bit in a fragmentation flag field in the header for each packet is set to a value that is arranged to prevent fragmentation of the packet en route; b. determining a maximum packet size for avoiding fragmentation in transmissions from a first security gateway to a second security gateway based on the received plurality of packets; and c. transmitting a feedback message to the first IPsec node from the second IPsec node with an indication of the maximum packet size [0125 - 0148].

8. Regarding Claim 28 Hamadeh teaches and describes an apparatus for facilitating reduction of a security threat in connection with transmission of an IP datagram having an IP header and an identification field in the IP header comprising: means for supplementing the identification field with at least one bit from another field of the IP header, whereby the security threat in connection with the transmission of the IP datagram is reduced [0125 - 0148].

9. Regarding Claim 29 Hamadeh teaches and describes an apparatus for formatting an IP datagram having an IP header comprising: means for determining identification information having a length greater than 16 bits associated with data to be sent in the IP datagram; means for inserting at least one bit of the identification information into an identification field of the header for the IP datagram; and means for inserting remaining bits of the identification information into at least one field of the header of the IP datagram other than the identification field [0125 - 0148].

10. Regarding Claim 38 Hamadeh teaches and describes an apparatus for formatting an IP datagram having an IP header comprising: means for determining a special value based on a secret shared with a destination node; and means for inserting at least a part of the special value into identification information carried by the header for the IP datagram, wherein a first portion of the identification information is included in an identification field and a second portion of the identification information is included in at least one other field of the header of the IP datagram [0125 - 0148].

11. Regarding Claim 45 Hamadeh teaches and describes an apparatus for facilitating fragmentation-free transmissions between two IPsec nodes implementing IPsec protocol, the apparatus comprising: means for transmitting a plurality of packets of differing size from a first one of the IPsec nodes to a second one of the IPsec nodes, each of the packets having an IP header, wherein a "Don't Fragment" (DF) bit in a fragmentation flag field in the header for each packet of the plurality is set to a value that is arranged to prevent fragmentation of the packet en route; and means for determining a maximum packet size for avoiding fragmentation in transmissions from the first IPsec node to the second IPsec node based on at least one response from the second IPsec node to the plurality of packets transmitted by the first IPsec node [0125 - 0148].

12. Regarding Claim 47 Hamadeh teaches and describes an apparatus for assembling a plurality of received IP datagrams each having an IP header comprising: means for assembling the plurality of received IP datagrams based on identification information contained in an

identification field of the header for each received IP datagram and at least one other field of the header for each received IP datagram, wherein the identification information for each one of the received IP datagrams does not include source address information, destination address information or protocol information for that received IP datagram [0125 - 0148].

13. Regarding Claim 49 Hamadeh teaches and describes an apparatus for assembling IP datagrams each having an IP header comprising: means for receiving a plurality of IP datagrams; means for extracting identification information from each of the plurality of IP datagrams, the identification information for each IP datagram comprising 16 bits of an identification field of the header for that IP datagram and at least one bit from at least one other field of the header for that IP datagram, the at least one bit not including source address information, destination address information or protocol information for the IP datagram; means for identifying a subset of the plurality of IP datagrams based on the identification information and at least one element selected from the group consisting of the source address information, the destination address information and the protocol information for each IP datagram from the subset; and means for assembling the subset of the plurality of IP datagrams into a message based on fragmentation offset information from a fragmentation offset field of the header for each IP datagram from the subset [0125 - 0148].

14. Regarding Claim 53 Hamadeh teaches and describes an apparatus for facilitating fragmentation-free transmissions between two IPsec nodes implementing IPsec protocol, the apparatus comprising: means for receiving a plurality of packets of differing size from a first one

of the IPsec nodes at a second one of the IPsec nodes, each of the packets having an IP header, wherein a "Don't Fragment" (DF) bit in a fragmentation flag field in the header for each packet from the plurality of packets is set to a value preventing fragmentation of the packet en route; means for determining a maximum packet size for avoiding fragmentation in transmissions from a first security gateway to a second security gateway based on the received plurality of packets; and means for transmitting a feedback message to the first IPsec node from the second IPsec node with an indication of the maximum packet size [0125 - 0148].

15. Regarding Claim 55 Hamadeh teaches and describes a computer-readable medium having stored thereon instructions, which when executed by a processor, cause the processor to perform a method for facilitating reduction of security threats in connection with transmission of an IP datagram having an IP header and an identification field in the IP header, the method comprising: supplementing the identification field of the IP header of the IP datagram with at least one bit from another field of the IP header, whereby the security threats in connection with the transmission of the IP datagram are reduced [0125 - 0148].

16. Regarding Claim 56 Hamadeh teaches and describes a computer-readable medium having stored thereon instructions, which when executed by a processor, cause the processor to perform a method for formatting an IP datagram having an IP header comprising: a. determining identification information having a length greater than 16 bits associated with data to be sent in the IP datagram; b. inserting at least one bit of the identification information into an identification field of the header for the IP datagram; and c. inserting the remaining bits of the

identification information into at least one field of the header of the IP datagram other than the identification field [0125 - 0148].

17. Regarding Claim 65 Hamadeh teaches and describes a computer-readable medium having stored thereon instructions, which when executed by a processor, cause the processor to perform a method for formatting an EP datagram having an IP header, the method comprising: a. determining a special value based on a secret shared with a destination node; and b. inserting at least a part of the special value into identification information carried by the header for the IP datagram, wherein a first portion of the identification information is included in an identification field and a second portion of the identification information is included in at least one other field of the header of the IP datagram [0125 - 0148].

18. Regarding Claim 72 Hamadeh teaches and describes a computer-readable medium having stored thereon instructions, which when executed by a processor, cause the processor to perform a method for facilitating fragmentation-free transmissions between two IPsec nodes implementing the IPsec protocol, the method comprising: a. transmitting a plurality of packets of differing size from a first IPsec node to a second IPsec node, wherein the "Don't Fragment" (DF) bit in the fragmentation flag field in the header for each packet of the plurality is set to a value that is arranged to prevent fragmentation of the packet en route; and b. determining a maximum packet size for avoiding fragmentation in transmissions from the first IPsec node to the second IPsec node based on at least one response from the second IPsec node to the plurality of packets transmitted by the first IPsec node [0125 - 0148].

19. Regarding Claim 74 Hamadeh teaches and describes a computer-readable medium having stored thereon instructions, which when executed by a processor, cause the processor to perform a method for assembling a plurality of received IP datagrams, the method comprising: assembling the plurality of received IP datagrams based on identification information contained in the identification field of the header for each received IP datagram and at least one other field of the header for each received IP datagram, wherein the identification information for each received IP datagram does not include source address information, destination address information or protocol information for that received IP datagram [0125 - 0148].

20. Regarding Claim 76 Hamadeh teaches and describes a computer-readable medium having stored thereon instructions, which when executed by a processor, cause the processor to perform a method for assembling IP datagrams, the method comprising: a. receiving a plurality of IP datagrams; b. extracting identification information from each of the plurality of IP datagrams, the identification information for each IP datagram comprising 16 bits of the identification field of the header for that IP datagram and at least one bit from at least one other field of the header for that IP datagram, the at least one bit not including source address information, destination address information or protocol information for the IP datagram; c. identifying a subset of the plurality of IP datagrams based on the identification information and at least one element selected from the group consisting of the source address information, the destination address information and the protocol information for each IP datagram from the subset; and d. assembling the subset of the plurality of IP datagrams into a message based on fragmentation

offset information from the fragmentation offset field of the header for each IP datagram from the subset of the plurality of IP datagrams [0125 - 0148].

21. Regarding Claim 80 Hamadeh teaches and describes a computer-readable medium having stored thereon instructions, which when executed by a processor, cause the processor to perform a method for facilitating fragmentation-free transmissions between two IPsec nodes implementing the IPsec protocol, the method comprising: a. receiving a plurality of packets of differing size from a first IPsec node at a second IPsec node, wherein the "Don't Fragment" (DF) bit in the fragmentation flag field in the header for each packet from the plurality of packets is set to a value preventing fragmentation of the packet en route; b. determining a maximum packet size for avoiding fragmentation in transmissions from the first security gateway to the second security gateway based on the received plurality of packets; and c. transmitting a feedback message to the first IPsec node from the second IPsec node with an indication of the maximum packet size [0125 - 0148].

22. Regarding Claim 82 Hamadeh teaches and describes a method for facilitating the reduction of a security threat in connection with the transmission of an IP datagram having an IP header and an identification field in the IP header comprising: supplementing the identification field of the IP header of the IP datagram with at least one bit from another field of the IP header, wherein the remaining bits of the another field contain an amount of information that is sufficient for an intermediate node or a receiving node to carry out the functionality normally corresponding to the another field [0125 - 0148].

23. Regarding Claim 84 Hamadeh teaches and describes a computer-readable medium having stored thereon instructions, which when executed by a processor, cause the processor to perform a method for facilitating fragmentation-free transmissions between two IPsec nodes implementing the IPsec protocol, the method comprising: supplementing the identification field of the IP header of the IP datagram with at least one bit from another field of the IP header, wherein the remaining bits of the another field contain an amount of information that is sufficient for an intermediate node or a receiving node to carry out the functionality normally corresponding to the another field [0125 - 0148].

24. Claims 2-10, 12-17, 19, 21, 23-25, 27, 30-37, 39-44, 46, and 48 are rejected applied as above rejecting Claim 12, 11, 18, 20, 22, 26, 28, 29, 38, 45, 49, 53, 56, 65, 72, 74, and 80. Furthermore, Hamadeh teaches

As per claim 3 further comprising transmitting the IP datagram ([0070]).

As per claim 4, the step of inserting the remaining bits of the identification information is carried out by inserting at least one of the remaining bits into a sub-network sub-field of at least one of a source address field and a destination address field of the header ([0127-0142])

As per claim 5, further comprising: d. inserting source address information for the IP datagram into the source address field of the header; e. inserting destination address information

for the IP datagram into the destination address field of the header; and f. inserting protocol information for the IP datagram into a protocol field of the header ([0127-0142]).

As per claim 6, the step of inserting the remaining bits of the identification information is carried out by inserting at least one of the remaining bits into a protocol field of the header ([0127-0142]).

As per claim 7, additionally comprising: d. inserting source address information for the IP datagram into the source address field of the header for the IP datagram; e. inserting destination address information for the IP datagram into the destination address field of the header for the IP datagram; and f. inserting protocol information for the IP datagram into the protocol field of the header for the IP datagram ([0127-0142]).

As per claim 8, the step of inserting the remaining bits of the identification information is carried out by inserting at least one of the remaining bits into a fragment offset field of the header ([0127-0142]).

As per claim 9, further comprising: d. inserting source address information for the IP datagram into a source address field of the header; e. inserting destination address information for the IP datagram into a destination address field of the header; and f. inserting protocol information for the IP datagram into a protocol field of the header ([0127-0142]).

As per claim 10, the step of inserting at least one bit is carried out by inserting 16 bits of the identification information into an identification field of the header ([0127-0142]).

As per claim 12, further comprising transmitting the IP datagram ([0070]).

As per claim 13, in the determining step the special value is additionally based on at least one element selected from the group consisting of source address information, destination address information and at least one bit from the identification field ([0127-0142]).

As per claim 14, the inserting step is carried out by placing the part of the special value into the identification field ([0127-0142]).

As per claim 15, further comprising: c. inserting at least another part of the special value into the at least one other field of the header for ([0127-0142]).

As per claim 16, the part of the special value inserted into the identification field has a bit length less than 16 bits and the method further comprises: c. determining additional identification information associated with the header for the IP datagram; and d. inserting at least part of the additional identification information into the identification field of the header for the IP datagram ([0127-0142]).

As per claim 17, further comprising: e. inserting at least another part of the additional identification information into a field of the header for the IP datagram other than the identification field ([0127-0142]).

As per claim 19, further comprising: c. transmitting at least one packet from the first IPsec node to the second IPsec node, wherein the packet size of the at least one packet is less than or equal to the maximum packet size ([0108-0113]).

As per claim 21, the at least one other field comprises at least one field selected from the group consisting of the sub-net subfield of at least one of the source address field and the destination address field of the header for each received IP datagram, the protocol field of the

header for each received IP datagram and the fragment offset field of the header for each received IP datagram ([0127-0142]).

As per claim 23, the at least one other field of the header for that IP datagram is selected from the group consisting of the sub-net subfield of at least one of the source address field and the destination address field of the header for that IP datagram, the protocol field of the header for that IP datagram and the fragmentation offset field of the header for that IP datagram ([0127-0142]).

As per claim 24, the identifying step comprises: e. determining a special value based on a secret shared with a source node; and f. identifying at least one IP datagram from the plurality as part of the subset based on the at least one IP datagram's containing the special value as part of the identification information for the at least one IP datagram ([0127-0142]).

As per claim 25, in the determining step the special value is additionally based on at least one element selected from the group consisting of the source address information, the destination address information and at least one bit from the identification field of the header for the at least one IP datagram ([0127-0142]).

As per claim 27, further comprising: d. receiving at least one packet from the first IPsec node at the second IPsec node after the transmitting step wherein the at least one packet has a packet size less than or equal to the maximum packet size ([0108-0113]).

As per claim 30, further comprising means for transmitting the IP datagram ([0070]).

As per claim 31, the means for inserting the remaining bits of the identification information insert at least one of the remaining bits into the sub-network sub-field of at least one

of the source address field and the destination address field of the header for the IP datagram ([0127-0142]).

As per claim 32, further comprising: means for inserting source address information for the IP datagram into the source address field of the header for the IP datagram; means for inserting destination address information for the IP datagram into the destination address field of the header for the IP datagram; and means for inserting protocol information for the IP datagram into the protocol field of the header for the IP datagram ([0127-0142]).

As per claim 33, the means for inserting the remaining bits of the identification information insert at least one of the remaining bits into the protocol field of the header for the IP datagram ([0127-0142]).

As per claim 34, additionally comprising: means for inserting source address information for the IP datagram into the source address field of the header for the IP datagram; means for inserting destination address information for the IP datagram into the destination address field of the header for the IP datagram; and means for inserting protocol information for the IP datagram into the protocol field of the header for the IP datagram ([0127-0142]).

As per claim 35, the means for inserting the remaining bits of the identification information insert at least one of the remaining bits into the fragment offset field of the header for the IP datagram ([0127-0142]).

As per claim 36, further comprising: means for inserting source address information for the IP datagram into the source address field of the header for the IP datagram; means for inserting destination address information for the IP datagram into the destination address field of

the header for the IP datagram; and means for inserting protocol information for the IP datagram into the protocol field of the header for the IP datagram ([0127-0142]).

As per claim 37, the means for inserting at least one bit insert 16 bits of the identification information into the identification field of the header for the IP datagram ([0127-0142]).

As per claim 39, further comprising means for transmitting the IP datagram ([0070]).

As per claim 40, the means for determining the special value bases the determination on at least one element selected from the group consisting of source address information, destination address information and at least one bit from the identification field of the header for the IP datagram ([0127-0142]).

As per claim 41, the means for inserting inserts the part of the special value into the identification field of the header for the IP datagram ([0127-0142]).

As per claim 42, further comprising: means for inserting at least another part of the special value into the at least one other field of the header for the IP datagram ([0127-0142]).

As per claim 43, the part of the special value inserted into the identification field has a bit length less than 16 bits and the apparatus further comprises: means for determining additional identification information associated with the header for the IP datagram; and means for inserting at least part of the additional identification information into the identification field of the header for the IP datagram ([0127-0142]).

As per claim 44, further comprising: means for inserting at least another part of the additional identification information into a field of the header for the IP datagram other than the identification field ([0127-0142]).

As per claim 46, further comprising: means for transmitting at least one packet from the first IPsec node to the second IPsec node, wherein the packet size of the at least one packet is less than or equal to the maximum packet size ([0108-0113]).

As per claim 48, the at least one other field comprises at least one field selected from the group consisting of the sub-net subfield of at least one of the source address field and the destination address field of the header for each received IP datagram, the protocol field of the header for each received IP datagram and the fragment offset field of the header for each received IP datagram ([0127-0142]).

As per claim 50, the at least one other field of the header for that IP datagram is selected from the group consisting of the sub-net subfield of at least one of the source address field and the destination address field of the header for that IP datagram, the protocol field of the header for that IP datagram, the protocol field of the header for that IP datagram and the fragmentation offset field of the header for that IP datagram ([0127-0142]).

As per claim 51, the means for identifying further comprises: means for determining a special value based on a secret shared with a source node; and means for identifying at least one IP datagram from the plurality as part of the subset based on the at least one IP datagram's containing the special value as part of the identification information for the at least one IP datagram ([0127-0142]).

As per claim 52, the means for determining additionally bases the determination on at least one element selected from the group consisting of the source address information, the destination address information and at least one bit from the identification field of the header for the at least one IP datagram ([0127-0142]).

As per claim 54, further comprising: means for receiving at least one packet from the first IPsec node at the second IPsec node after the transmitting step wherein the at least one packet has a packet size less than or equal to the maximum packet size ([0108-0113]).

As per claim 57, the method further comprises transmitting the IP datagram ([0070]).

As per claim 58, the step of inserting the remaining bits of the identification information is carried out by inserting at least one of the remaining bits into the sub-network sub-field of at least one of the source address field and the destination address field of the header for the IP datagram ([0127-0142]).

As per claim 59, the method further comprises: d. inserting source address information for the IP datagram into the source address field of the header for the IP datagram; e. inserting destination address information for the IP datagram into the destination address field of the header for the IP datagram; and f. inserting protocol information for the IP datagram into the protocol field of the header for the IP datagram ([0127-0142]).

As per claim 60, the step of inserting the remaining bits of the identification information is carried out by inserting at least one of the remaining bits into the protocol field of the header for the IP datagram ([0127-0142]).

As per claim 61, the method further comprises: d. inserting source address information for the EP datagram into the source address field of the header for the IP datagram; e. inserting destination address information for the IP datagram into the destination address field of the header for the IP datagram; and f. inserting protocol information for the IP datagram into the protocol field of the header for the IP datagram ([0127-0142]).

As per claim 62, the step of inserting the remaining bits of the identification information is carried out by inserting at least one of the remaining bits into the fragment offset field of the header for the IP datagram ([0127-0142]).

As per claim 63, the method further comprises: d. inserting source address information for the IP datagram into the source address field of the header for the IP datagram; e. inserting destination address information for the IP datagram into the destination address field of the header for the IP datagram; and f. inserting protocol information for the IP datagram into the protocol field of the header for the IP datagram ([0127-0142]).

As per claim 64, the step of inserting at least one bit is carried out by inserting 16 bits of the identification information into the identification field of the header for the IP datagram ([0127-0142]).

As per claim 66, the method further comprises transmitting the IP datagram ([0070]).

As per claim 67, wherein in the determining step in the method the special value is additionally based on at least one element selected from the group consisting of source address information, destination address information and at least one bit from the identification field of the header for the IP datagram ([0127-0142]).

As per claim 68, the inserting step is carried out by placing the part of the special value into the identification field of the header for the IP datagram ([0127-0142]).

As per claim 69, the method further comprises: c. inserting at least another part of the special value into the at least one other field of the header for the IP datagram ([0127-0142]).

As per claim 70, the at least part of the special value inserted into the identification field has a bit length less than 16 bits and the method further comprises: c. determining additional

identification information associated with the header for the IP datagram; and d. inserting at least part of the additional identification information into the identification field of the header for the IP datagram ([0127-0142]).

As per claim 71, the method further comprises: e. inserting at least another part of the additional identification information into a field of the header for the IP datagram other than the identification field ([0127-0142]).

As per claim 73, the method further comprises: c. transmitting at least one packet from the first IPsec node to the second IPsec node, wherein the packet size of the at least one packet is less than or equal to the maximum packet size ([0108-0113]).

As per claim 75, the at least one other field comprises at least one field selected from the group consisting of the sub-net subfield of at least one of the source address field and the destination address field of the header for each received IP datagram, the protocol field of the header for each received IP datagram and the fragment offset field of the header for each received IP datagram ([0127-0142]).

As per claim 77, the at least one other field of the header for that IP datagram is selected from the group consisting of the sub-net subfield of at least one of the source address field and the destination address field of the header for that IP datagram, the protocol field of the header for that IP datagram and the fragmentation offset field of the header for that IP datagram ([0127-0142]).

As per claim 78, the identifying step in the method comprises: e. determining a special value based on a secret shared with a source node; and f. identifying at least one IP datagram from the plurality as part of the subset based on the at least one IP datagram's containing the

special value as part of the identification information for the at least one IP datagram ([0127-0142]).

As per claim 79, in the determining step in the method the special value is additionally based on at least one element selected from the group consisting of the source address information, the destination address information and at least one bit from the identification field of the header for the at least one IP datagram ([0127-0142]).

As per claim 81, the method further comprises: receiving at least one packet from the first IPsec node at the second IPsec node after the transmitting step wherein the at least one packet has a packet size less than or equal to the maximum packet size ([0108-0113]).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SYED ZIA whose telephone number is (571)272-3798. The examiner can normally be reached on 9:00 to 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

sz
March 2, 2009
/Syed Zia/
Primary Examiner, Art Unit 2431